ООО «ЭЛЕТЕК»

Программный комплекс

«Контроль-ПК»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Москва 2024

Содержание

Список сокращений

АРМ – рабочее место оператора;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

HTTPS (англ. HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS;

HTTPS-сервер - компьютер, подключенный к локальной или глобальной сети, используемый для хранения информации, а также её передачи по протоколу HTTPS;

TLS (англ. Transport Layer Security — безопасность транспортного уровня), как и его предшественник SSL (англ. Secure Sockets Layer — уровень защищённых сокетов) — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет.

Термины и определения

Исследуемый компьютер — средство вычислительной техники, с которого выполняется копирование данных.

Исследующий компьютер – средство вычислительной техники, предназначенное для подготовки программного комплекса к работе и распаковывания скопированных данных.

Введение

Настоящее руководство предназначено для пользователей программного комплекса «Контроль-ПК».

Руководство содержит сведения о назначении программного комплекса, его устройстве и комплектности. Кроме того, в руководстве изложено подробное описание основных операций, выполняемых в соответствии с целевым назначением комплекса.

1. Общие сведения

В настоящем руководстве для удобства работы пользователя принята двухзначная нумерация таблиц и рисунков в рамках каждого из разделов.

В тексте руководства используются следующие способы выделения шрифтом элементов интерфейса:

Таблица 1.1

Тип выделенного текста	*Принятый способ выделения*
имена папок, жестких дисков	**ПРОПИСНЫЕ БУКВЫ, полужирный шрифт**
имена окон, пункты меню	**С прописной буквы, полужирный шрифт**
имена кнопок	**[В КВАДРАТНЫХ СКОБКАХ], полужирный шрифт**
имена клавиш	**{В ФИГУРНЫХ СКОБКАХ}, полужирный шрифт**
данные, вводимые пользователем	`Courier New`, обычный шрифт

1.1 Назначение программного комплекса

Программный комплекс предназначен для контроля действий пользователей и копирования информации с ЭВМ, работающих под управлением операционных систем семейства Windows. Комплекс может быть использован для контроля действий сотрудников предприятий в рамках расследований инцидентов информационной безопасности, поиска инсайдеров и предотвращения утечек информации.

1.2 Состав программного комплекса

Комплекс «Контроль-ПК» предусматривает модульное расширение функционала В текущей версии реализованы функции сканирования и копирования файлов по предварительно заданным маскам имени файла или пути к файлу. Найденные методом автоматического сканирования файлы и готовые к отправке данные на исследуемом компьютере кодируются, разбиваются на фрагменты и загружаются на выделенный сервер по защищенному протоколу HTTPS. Сервер настраивается сотрудниками разработчика программного комплекса – ООО «Элетек». Данные с сервера скачиваются на рабочее место оператора также с использованием протокола HTTPS.

В текущей версии комплекса представлен функционал по копированию файлов по заданной маске, получению снимков экрана, сохранению клавиатурных последовательностей на протяжении всего сеанса работы исследуемого ПК.

Комплекс состоит из следующих модулей:

– модуль-агент (далее – агент) – устанавливается в ОС исследуемого компьютера, используется для контроля действий пользователя и копирования информации;

– модуль инсталляции – используется для установки агента в ОС исследуемого компьютера;

– управляющий модуль – предназначен для подготовки агента к установке, для дистанционного приема и обработки результатов функционирования агента, а также для дистанционного управления агентом.

Также в состав комплекса входит серверная составляющая, которая настраивается и обслуживается компанией-разработчиком.

2. Описание операций

К основным операциям относятся: подготовка агента к применению, формирование и загрузка задания на копирование данных, установка агента, сбор информации на сервере, копирование данных из исследуемого компьютера и их распаковывание, удаление агента.

2.1 Подготовка агента к применению

Для подготовки агента к применению по назначению выполните следующие действия:

1. Включите исследующий компьютер. На рабочем столе должна отобразиться иконка с именем программы **ControlPC.exe**. Если иконка не отображается, то установите рабочую программу из комплекта поставки на исследующий компьютер, используя стандартные средства установки программ ОС Windows.

2. Подсоедините к исследующему компьютеру флеш-накопитель. В окне **Компьютер** ОС Windows в разделе **Устройства со съемными носителями** отобразится вновь подключенное устройство с присвоенным ему именем тома.

3. Запустите рабочую программу **ControlPC.exe**, установив курсор на иконку и дважды нажав на левую кнопку мыши. На экране исследующего компьютера отобразится главное окно программы **Контроль-ПК** (Рисунок 1.1).

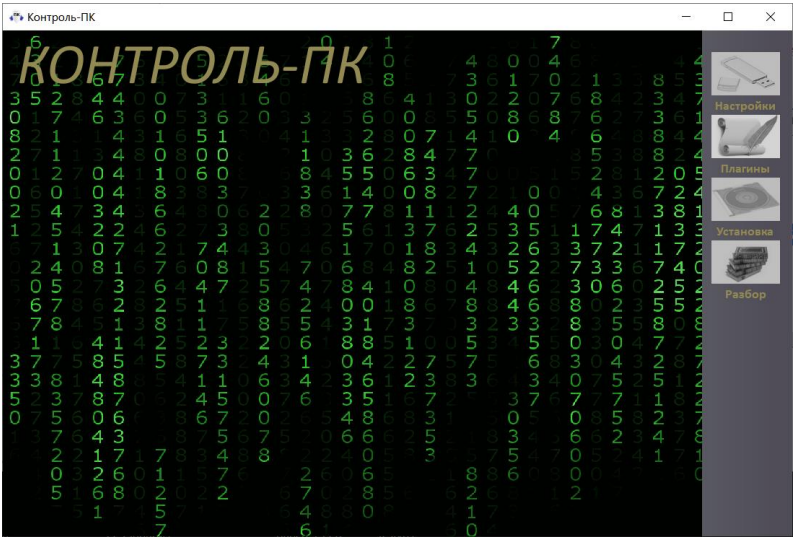

Рисунок 1.1

Главное окно содержит панель инструментов, расположенную вертикально в правой части окна. На панели инструментов размещены управляющие кнопки, состав и назначение которых представлены в таблице 2.1.

Таблица 2.1

Имя кнопки	***Назначение***
[Настройки]	Настройка параметров соединения сервера, создание или выбор профиля задания на копирование данных
[Плагины]	Создание задания с выбором необходимых плагинов
[Установка]	Загрузка агента и модуля инсталляции (с параметрами подключения к HTTPS-серверу) на флеш-накопитель
[Разбор]	Выполнение операций распаковывания полученных данных

2.2 Настройка параметров

Для функционирования агента необходимо произвести корректную настройку.

Для настройки параметров потребуется вкладка **Настройки**, расположенная в правой части окна интерфейса программы (Рисунок 1.1).

2.2.1 Вкладка «Настройки»

Во вкладке «**Настройки»** (рисунок 2.2.1) осуществляется настройка подключения к серверу, выбор пользователей, а также отображается активность функционирования агента.

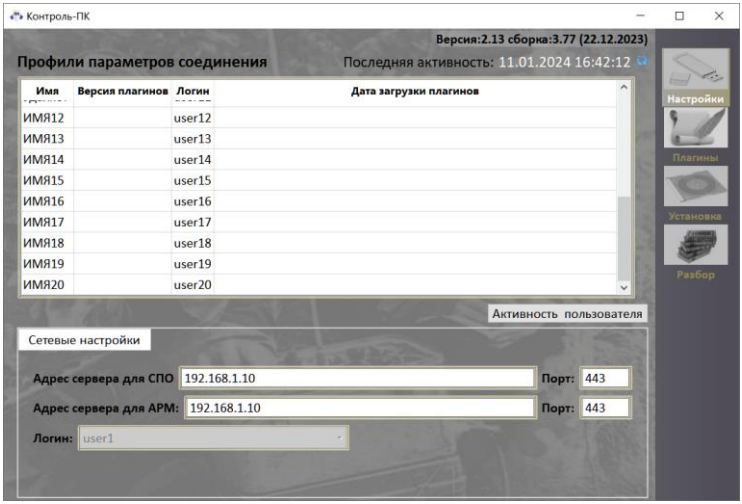

Рисунок 2.2.1

Элементы интерфейса, их имена и назначение представлены в таблице 2.2.1

Таблица 2.2.1

Элемент интерфейса	*Имя элемента*	*Назначение*
Таблица данных	**Профили параметров соединения**	Выбор и создание профиля задания
Кнопка	**Активность пользователя**	Просмотр информации о работе программного обеспечения по выбранному пользователю
Форма	**Сетевые настройки**	Определение сетевых настроек
Поле редактирования	**Адрес сервера для СПО**	Определение IP-адреса HTTPS-сервера для агента
Информационное поле	**Порт**	Определение порта HTTPS-сервера
Поле редактирования	**Адрес сервера для АРМ**	Определение IP-адреса HTTPS-сервера для исследуемого компьютера
Поле выбора	**Логин**	Определение имени пользователя для подключения к HTTPS-серверу

2.2.1.1 Профили параметров соединения

ВНИМАНИЕ! ВАЖНО!

В минимальной версии поставки в программе предустановлен IP адрес тестового сервера для демонстрации работы и предусмотрен один пользователь с именем **ДЕМО** (логин **user10**).

Для настройки аганта в окне «**Настройки»** необходимо выбрать профиль и, при необходимости переименовать его, нажав правую кнопку мыши в выбранном профиле в строке блока **«Профили параметров соединения».**

Появится предложение **«Переименовать»** (рисунок 2.2.1.1).

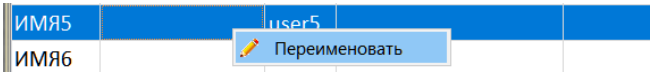

Рисунок 2.2.1.1

Далее присваиваем имя профилю, используя окно ввода данных (рисунок 2.2.1.2).

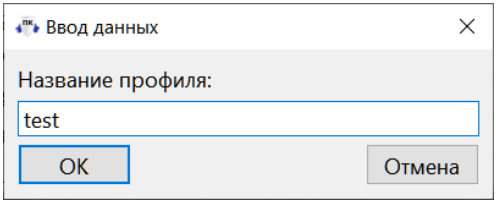

Рисунок 2.2.1.2

Вводим название `test`. В результате, в блоке **«Профили параметров соединения»** получаем созданный профиль «test. Отображение профиля на рисунке 2.2.1.3

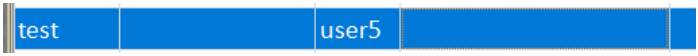

Рисунок 2.2.1.3

2.2.1.2 Настройки агента

В блоке **«Сетевые настройки»** во вкладке **«Настройки»** необходимо указать настройки для подключения к HTTPS-серверу (IP-адрес, порт).

При вводе данных в поле «`Адрес сервера для СПО`» необходимо ввести IP-адрес сервера, настроенного на работу в глобальной

сети интернет, т.е. указать «внешний» адрес сервера, отличный от диапазона адресов внутренней сети, таких как *10.10.10.10* или *192.168.1.10*.

Внимание!

Сервер должен иметь прямое подключение к глобальной сети Интернет (белый адрес).

Если работа агента предполагает сбор информации только в пределах локальной сети, в поле «Адрес сервера для СПО» необходимо ввести адрес из диапазона адресов имеющейся развернутой локальной сети.

В поле «Адрес сервера для АРМ» указываем локальный IP-адрес сервера. К примеру *192.168.0.10*. Данное действие необходимо в случае, если АРМ оператора подключен напрямую или по внутренней сети ко второму сетевому адаптеру сервера.

В случае, если управление агентом производится через глобальную сеть Интернет по первому интерфейсу, то необходимо указать только «белый» IP-адрес. В этом случае адреса полей «Адрес сервера для СПО» и «Адрес сервера для АРМ» совпадут (рисунок 2.2.1.12).

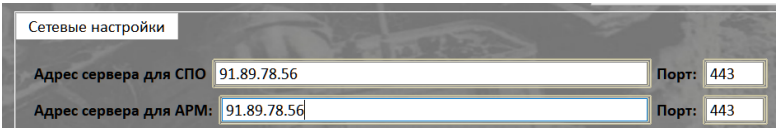

Рисунок 2.2.1.12

Пример настройки сервера при подключении АРМ оператора напрямую или через внутреннюю сеть с использованием второго адаптера сервера (рисунок 2.2.1.13).

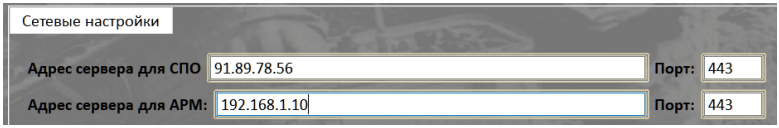

Рисунок 2.2.1.13

На рисунке 2.2.1.14 представлен пример настройки сервера для работы только в локальной сети:

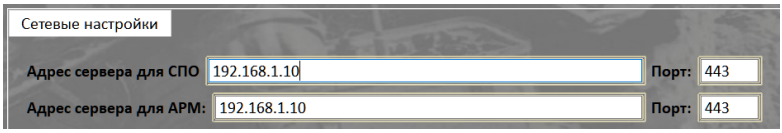

Рисунок 2.2.1.14

Далее необходимо выбрать логин пользователя.

Внимание!

Работа с комплексом «Контроль-ПК» возможна при одновременном подключении не более двадцати пользователей (user1, user2, user3, …, user20).

Комплекс способен функционировать как с одним пользователем, выбранным из списка, так и с несколькими сразу. Логин пользователей не изменяется и не может быть редактирован оператором в ходе настройки программы. Пароль должен быть «сложным», содержать заглавные и прописные буквы, цифры и спецсимволы.

2.2.1.3 Активность пользователя

На рисунке 2.2.1.15 представлено отображение кнопки **[Активность пользователя]**.

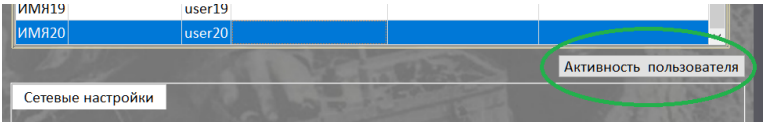

Рисунок 2.2.1.15

При нажатии на кнопку **[Активность пользователя]**, оператор получает информацию о состоянии сервера, активности пользователя, а также об объеме загруженных пользователем данных и общего свободного объема на сервере. На рисунке 2.2.1.16 представлен внешний вид окна **Активность пользователя**.

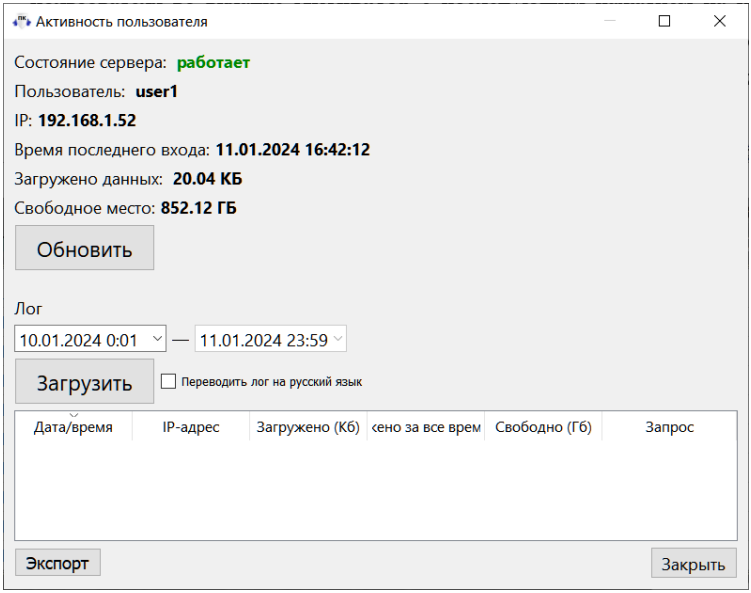

Рисунок 2.2.1.16

Строка **Состояние сервера** отображает статус работы сервера. Статус функционирующего сервера будет отображен зеленой надписью работает, в том время, как неработающий сервер будет отображен красной надписью недоступен.

Внимание!

Для корректного отображения информации о состоянии сервера необходимо сетевое подключение между АРМ оператора и сервера в локальной или глобальной сетях.

В случае недоступности сервера или некорректного ввода пароля пользователя во вкладке **Настройки** с последующим нажатием на кнопку

[Активность пользователя], состояние сервера будет недоступен, указан пользователь, остальные поля будут неинформативны. Отображение ситуации на рисунке 2.2.1.17.

Рисунок 2.2.1.17

В случае работающего доступного сервера состояние сервера будет работает, указан пользователь, от имени которого создано задание и IP-адрес исследуемого компьютера, с которого происходит получение информации для последующего разбора и анализа. Также на рисунке 2.2.1.16 отображено время последней активности агента.

На этом же рисунке отображен объем данных, находящихся в директории *user1*. При смене пользователя в окне **Настройки** и дальнейшим нажатием на **[Активность пользователя]** будет выводиться информация о выбранном пользователе, его объеме загруженных данных, активности и IP-адресе.

При нажатии на кнопку **[Обновить]** произойдет обновление информации о выбранном пользователе.

Информация в строке **Свободное место** отображает информацию об оставшемся свободном месте на жестком диске сервера. Соответственно эта информация будет общая для любого пользователя.

Если свободное место для предоставляемых данных заканчивается, то рядом с цифровым значением оставшегося объема появится надпись мало места (рисунок 2.2.118). При наведении на «знак вопроса» отобразится соответствующее сообщение с рекомендациями.

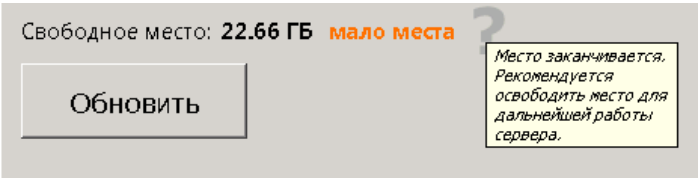

Рисунок 2.2.1.18

Если свободный объем полностью исчерпан, то появится надпись место закончилось, передача данных из исследуемого компьютера на сервер приостановится (рисунок 2.2.1.19). При наведении на «знак вопроса» отобразится соответствующее сообщение.

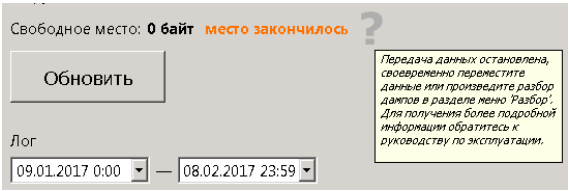

Рисунок 2.2.1.19

В этих случаях необходимо освободить жесткий диск от данных. Подробная инструкция описана в разделе 2.5.

В случае приостановки передачи данных при заполнении жесткого диска или недоступности сервера по сети данные начнут накапливаться в

директории на исследуемом компьютере. При вновь доступном в сети сервере и при наличии свободного объема на жестком диске, данные будут переданы на сервер.

Особенность.

При работе агента в глобальной сети в строке **IP-адрес** будет указан внешний адрес, полученный исследующим компьютером при выходе в сеть. Соответственно, если работа с нескольких ПК происходит через роутер, имеющий выход в интернет, то у каждого из этих пользователей будет один и тот же внешний IP-адрес. В случае задания с компьютерами, подключенными к разным сетевым сегментам, каждому пользователю будет «выделен» свой внешний IP-адрес, который в последствии будет отображен в строке **IP-адрес**.

Если работа агента происходит в пределах локальной сети, то у каждого пользователя будет отображен свой IP-адрес из диапазона локальной сети (*пример 192.168.1.24, 10.10.10.28*).

Окно **Активность пользователя** также отображает сохраненную информацию о подключениях в течение одного месяца. Данная информация представлена в поле **Лог** (рисунок 2.2.1.20).

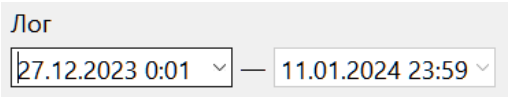

Рисунок 2.2.1.20

Выбрав необходимый временной интервал для отображения информации, необходимо нажать кнопку **[Загрузить]**. На экран будет выведена информация о работе агента (рисунок 2.2.1.21).

Дата/время	IP-адрес	Загружено (Кб)	Загружено за все время (Мб)	Свободно (Гб)
11.01.2024 16:40	192.168.1.52	0	22374,2	852,12
11.01.2024 16:27	192.168.1.52	0	22374,2	852,12

Рисунок 2.2.1.21

Нажатие на кнопку **[Экспорт]** позволит сохранить имеющуюся статистику по работе агента в выбранную оператором директорию.

2.3 Формирование и загрузка задания на копирование данных

Для формирования и загрузки заданий необходимо перейти на вкладку **Плагины** (рисунок 2.3.1), расположенную в правой части окна программы. Предварительно потребуется выполнить настройки конфигурации агента. Шаги по необходимой настройке описаны в разделе 2.2.

Рисунок 2.3.1

На рисунке 2.3.2 представлен общий вид вкладки Плагины.

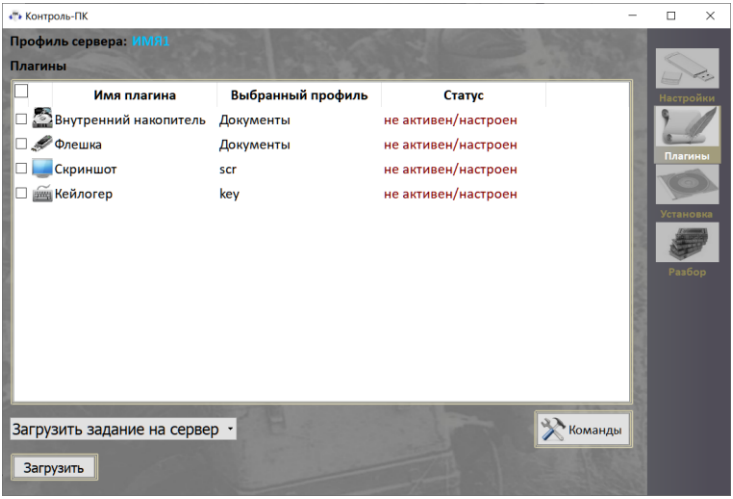

Рисунок 2.3.2

Элементы интерфейса окна **Плагины**, их имена и назначение представлены в таблице 2.3.1.

Таблица 2.3.1

Элемент интерфейса	***Имя элемента***	***Назначение***
Таблица данных	**Плагины**	Отображение списка доступных для настройки плагинов.
Кнопка	**Загрузить задания на сервер**	Загрузка конфигурационных данных модулей с АРМ оператора на сервер
Кнопка	**Команды**	Список доступных команд управления

Одним из элементов на вкладке **Плагины** является информационная панель (рисунок 2.3.3) с указанием выбранного профиля сервера. Операции по настройке и выбору профиля описаны в разделе 2.2.1.1. При нажатии на выбранный профиль (*test*) программа переключится на вкладку **Найстройки** для уточнения или изменения настроек сервера.

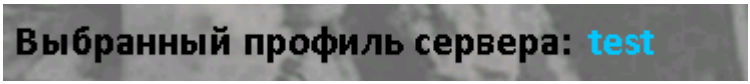

Рисунок 2.3.3

2.3.1 Формирование задания

На изображении содержимого вкладки **Плагины** (рисунок 2.3.1.1) представлен функционал по конфигурации модулей, необходимых для формирования задания для работы агента.

Рисунок 2.3.1.1

В программном комплексе представлены следующие модули (плагины):

1. Плагин «Внутренний накопитель»;
2. Плагин «Флешка»;

3. Плагин «Скриншот»;
4. Плагин «Кейлогер»;

Функционал каждого модуля будет описан подробно и представлен в настоящем руководстве.

В верхней части окна **Плагины** размещен чекбокс необходимый для включения и отключения оператором всех модулей при формировании задания на загрузку агента. Для выбора определенного плагина можно воспользоваться чекбоксом, расположенным непосредственно перед каждым плагином (рисунок 2.3.1.2).

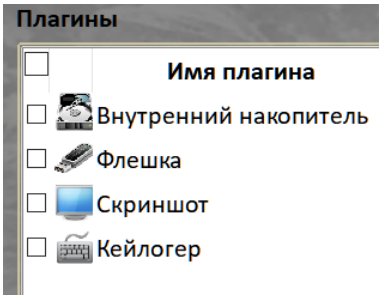

Рисунок 2.3.1.2

Двойной клик по выбранному плагину откроет окно настройки модуля, необходимой для формирования задания. Подробное описание настройке каждого плагина представлено ниже.

2.3.1.1 Плагин «Внутренний накопитель»

Активируем плагин **Внутренний накопитель** путем добавления флажка напротив модуля. Совершаем двойное нажатие левой кнопкой мыши

на элемент интерфейса **Внутренний накопитель**. Откроется окно с настройками модуля (рисунок 2.3.1.3).

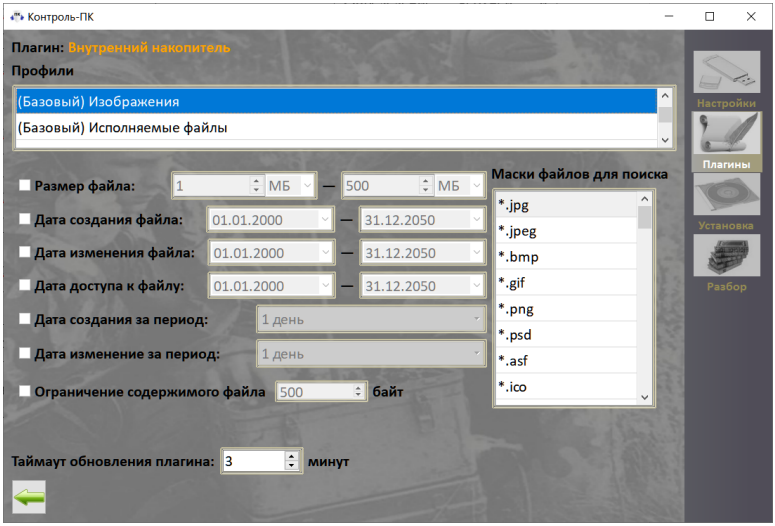

Рисунок 2.3.1.3

В окне настройки плагина «**Внутренний накопитель»** (рисунок 2.3.1.3) отображены элементы интерфейса для создания конфигурации модуля, их имена и назначение. Информация представлена в таблице 2.3.1.1.

Таблица 2.3.1.1.

Элемент интерфейса	***Имя элемента***	***Назначение***
Таблица данных	**Профили**	Формирование профиля плагина

Элемент интерфейса	*Имя элемента*	*Назначение*
Таблица данных	**Маски файлов для поиска**	Формирование выбора форматов файлов для копирования. Возможно указание масок путей к файлам.
Флаговая кнопка с полем редактирования	**Размер файла**	Определение верхней и нижней границы размера копируемого файла
Флаговая кнопка с полем редактирования	**Дата создания файла**	Определение верхней и нижней границы даты создания копируемого файла.
Флаговая кнопка с полем редактирования	**Дата изменения файла**	Определение верхней и нижней границы даты изменения копируемого файла
Флаговая кнопка с полем редактирования	**Дата доступа к файлу**	Определение верхней и нижней границы даты открытия копируемого файла
Флаговая кнопка с полем редактирования	**Ограничение содержимого файла**	Определение числа байт файла, которое следует скопировать. Если флаговая кнопка не выбрана, то файл копируется целиком
Поле редактирования	**Таймаут обновления плагина**	Задание периода обновления конфигурации
Кнопка	**Назад**	Переход в меню «Плагины» с сохранением внесенных изменений

Данный модуль необходим для отправки на сервер файлов, находящихся на жестком диске исследуемого компьютера.

Для настройки плагина «**Внутренний накопитель»** необходимо выбрать ранее созданный профиль из представленных по умолчанию (рисунок 2.3.1.4)

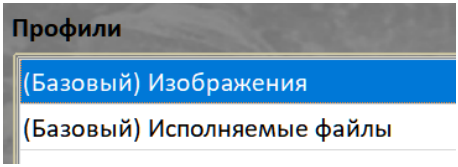

Рисунок 2.3.1.4

При работе с профилями по умолчанию автоматически добавляются **Маски файлов для поиска**, соответствующие выбранному профилю. Для редактирования оператором будут доступны опции **Ограничение содержимого файла** и **Таймаут обновления плагина**.

Для создания нового профиля необходимо нажать правую кнопку мыши в свободной строке блока **«Профили»**. Появится предложение **«Добавить»** (рисунок 2.3.1.5).

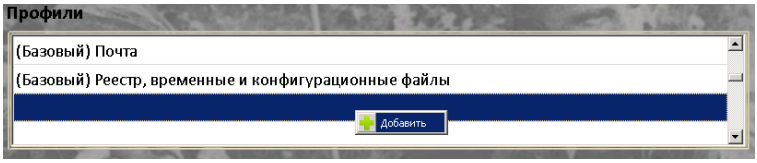

Рисунок 2.3.1.5

Далее присваиваем имя новому профилю, используя окно ввода данных (рисунок 2.3.1.6).

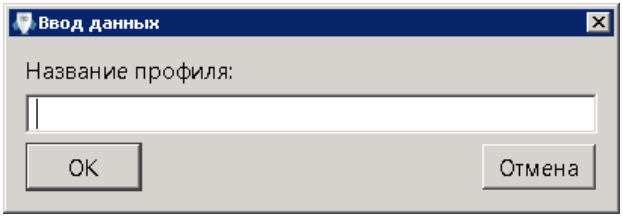

Рисунок 2.3.1.6

Вводим название `Внутренний накопитель` и нажимаем **[ОК]**. В результате, в блоке **«Профили»** получаем созданный профиль «Внутренний накопитель». Отображение профиля на рисунке 2.3.1.7.

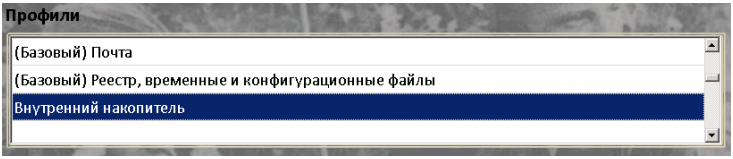

Рисунок 2.3.1.7

Также возможно делать копии базовых профилей с дальнейшим изменением копий при необходимости. Для этого, нажимая правой кнопкой мыши по профилю и вызывая контекстное меню, необходимо выбрать «Создать копию» (рисунок 2.3.1.8).

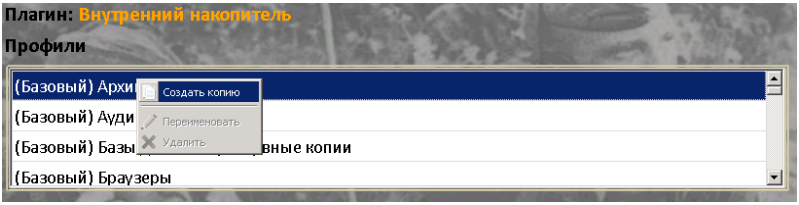

Рисунок 2.3.1.8

В появившемся окне **Ввод данных** (рисунок 2.3.1.9) задаем имя скопированному профилю и нажимаем **[ОК]**. Профиль будет добавлен в общий список.

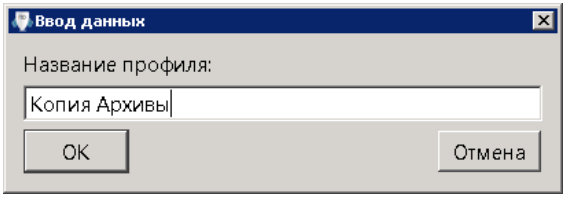

Рисунок 2.3.1.9

Далее необходимо произвести настройку выбранного профиля. Выбрать созданный профиль «Внутренний накопитель». Затем произвести двойное нажатие по свободной строке в блоке **Маски файлов для поиска**. Откроется окно ввода данных (рисунок 2.3.1.10). Вводим необходимую маску в таком формате: `*.jpg` и нажимаем **[OK]**.

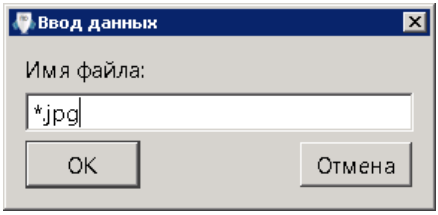

Рисунок 2.3.1.10

В случае необходимости копирования или удаления добавленной маски необходимо нажать правой кнопкой мыши на маску и выполнить соответствующее действие в контекстном меню (рисунок 2.3.1.11).

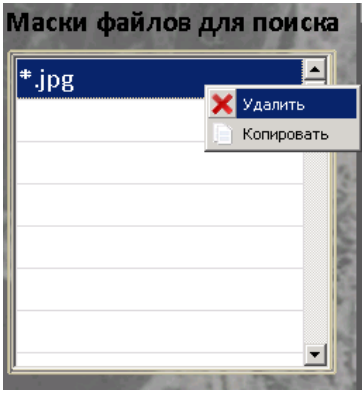

Рисунок 2.3.1.11

В случае необходимости удаления (рисунок 2.3.1.12) программа откроет следующее окно для подтверждения действия. Нажимаем кнопку **[Да]** для выполнения выбранного действия или **[Нет]** для отмены операции с добавленными масками поиска.

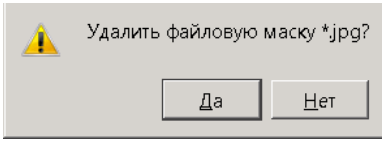

Рисунок 2.3.1.12

В случае необходимости копирования (рисунок 2.3.1.13) программа запомнит скопированные маски и при нажатии правой кнопкой мыши по свободной строке в блоке маски файлов для поиска предложит вставить скопированную маску.

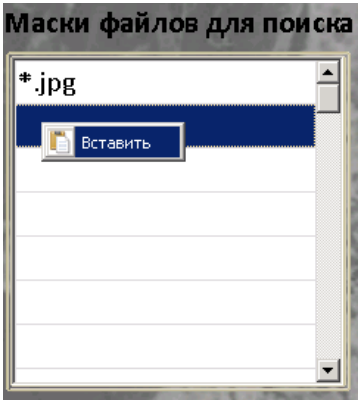

Рисунок 2.3.1.13

Маски могут копироваться по одной или группами из других доступных базовых профилей.

Вставлять маски можно только в созданный оператором профиль. Удаление или изменение масок при использовании базового профиля невозможно.

После добавления необходимых масок поиска необходимо отметить нужные для работы флаговые кнопки. К выбору предоставлены:

1. Размер файла.

Здесь указывается диапазон размеров файлов для поиска для дальнейшего копирования на сервер.

2. Дата создания файла.

В этой строке указывается временной диапазон для поиска файлов по дате создания для дальнейшего копирования на сервер.

3. Дата изменения файла.

В этой строке указывается временной диапазон для поиска файлов по дате изменения для дальнейшего копирования на сервер.

4. Дата доступа к файлу.

В этой строке указывается временной диапазон для поиска файлов по дате доступа к файлу для дальнейшего копирования на сервер.

Активируя флаговую кнопку **Ограничение содержимого файла** оператору необходимо задать размер файла в байтах. Согласно указанному размеру будет копироваться часть файла, начиная с «начала».

Пример.

Указан размер файла 500 байт (рисунок 2.3.1.14).

Рисунок 2.3.1.14

В результате работы агента был найден файл с расширением *.mkv* размером *1500Мб*. В этом случае при разборе данных с сервера будет распакован только фрагмент этого файла размером *500 байт*.

Данная опция нужна для предварительного анализа данных на исследуемом компьютере.

При выставлении в поле **Ограничение содержимого файла** размера равного *0 байт*, плагин будет работать в режиме **«Структура каталогов»**. На сервер будут скопированы все файлы нулевого размера с сохранением директории хранения и имени. Для этого также необходимо назначить маску *.* в блоке **Маски файлов для поиска**.

Выставляя значение в минутах в поле **Таймаут обновления плагина** (рисунок 2.3.1.15), оператор задает временной интервал обновления конфигурационных файлов плагина **Внутренний накопитель**. При наличии загруженной на сервер новой конфигурации для текущего модуля по истечению указанного времени произойдет замена имеющейся конфигурации на сервере.

Рисунок 2.3.1.15

По окончанию настроек необходимо нажать кнопку **[Назад]** для сохранения введенных настроек и возврата в основное меню настройки плагинов. Отображение кнопки и **[Назад]** представлено на рисунке 2.3.1.16.

Рисунок 2.3.1.16

Настройка плагина завершена. Конфигурация готова к загрузке на сервер.

2.3.1.2 Плагин «Флешка»

Активируем плагин **Флешка** путем добавления флажка напротив модуля. Совершаем двойное нажатие левой кнопкой мыши на элемент

интерфейса **Флешка**. Откроется окно с настройками модуля (рисунок 2.3.1.17).

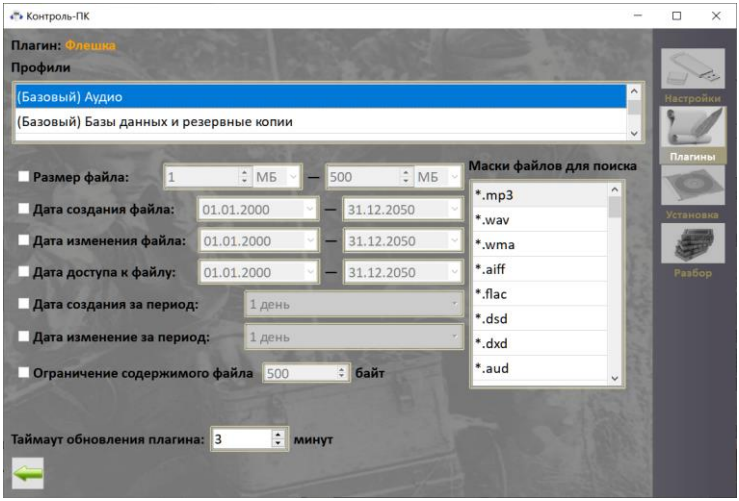

Рисунок 2.3.1.17

В окне настройки плагина «**Флешка»** (рисунок 2.3.1.17) отображены элементы интерфейса для создания конфигурации модуля, их имена и назначение представлены в таблице 2.3.1.2.

Таблица 2.3.1.2

Элемент Интерфейса	***Имя элемента***	***Назначение***
Таблица данных	**Профили**	Формирование профиля плагина
Таблица данных	**Маски файлов для поиска**	Формирование выбора форматов файлов для копирования. Возможно указание масок путей к файлам.

Элемент Интерфейса	*Имя элемента*	*Назначение*
Флаговая кнопка с полем редактирования	**Размер файла**	Определение верхней и нижней границы размера копируемого файла
Флаговая кнопка с полем редактирования	**Дата создания файла**	Определение верхней и нижней границы даты создания файла.
Флаговая кнопка с полем редактирования	**Дата изменения файла**	Определение верхней и нижней границы даты изменения файла
Флаговая кнопка с полем редактирования	**Дата доступа к файлу**	Определение верхней и нижней границы даты открытия файла
Флаговая кнопка с полем редактирования	**Ограничение содержимого файла**	Определение числа байт файла, которое следует скопировать. Если флаговая кнопка не выбрана, то файл копируется целиком
Поле редактирования	**Таймаут обновления плагина**	Задание периода обновления конфигурации
Кнопка	**Назад**	Переход в меню «Плагины» с сохранением внесенных изменений

Данный модуль необходим для отправки файлов, находящихся на подключенном к исследуемому компьютеру внешнем USB-накопителе.

Для настройки плагина **«Флешка»**, по аналогии с плагином **Внутренний накопитель**, необходимо выбрать ранее созданный профиль из представленных по умолчанию (рисунок 2.3.1.18)

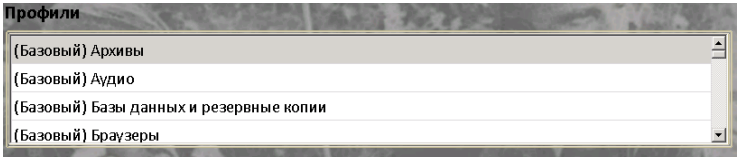

Рисунок 2.3.1.18

При работе с профилями по умолчанию автоматически добавляются **Маски файлов для поиска** соответствующие выбранному профилю. Для редактирования оператором будут доступны опции **Ограничение содержимого файла** и **Таймаут обновления плагина**.

Для создания нового профиля можно воспользоваться инструкцией представленной в разделе 2.3.1.1.

Далее необходимо произвести настройку выбранного профиля. Выбрать созданный профиль «Флешка». Затем произвести операции по созданию масок файлов для поиска. Подробная инструкция по работе с масками представлена в разделе 2.3.1.1.

После добавления необходимых масок поиска необходимо отметить нужные для работы флаговые кнопки. К выбору предоставлены:

1. Размер файла.

Здесь указывается диапазон размеров файлов для поиска и дальнейшего копирования на сервер.

2. Дата создания файла.

В этой строке указывается временной диапазон для поиска файлов по дате создания.

3. Дата изменения файла.

В этой строке указывается временной диапазон для поиска файлов по дате изменения.

4. Дата доступа к файлу.

В этой строке указывается временной диапазон для поиска файлов по дате доступа к файлу.

Активируя флаговую кнопку **Ограничение содержимого файла** оператору необходимо задать размер файла в байтах. Согласно указанному размеру будет копироваться часть файла, начиная с «начала».

Пример.

Указан размер файла 500 байт (рисунок 2.3.1.19).

Рисунок 2.3.1.19

В результате работы агента был найден файл с расширением *.mkv* размером *1500Мб*. В этом случае при разборе данных с сервера будет распакован только фрагмент этого файла размером *500 байт*.

Данная опция нужна для предварительного анализа данных на исследуемом компьютере.

При выставлении в поле **Ограничение содержимого файла** размера равного *0 байт*, плагин будет работать в режиме **«Структура файлов»**. На сервер будут скопированы все файлы нулевого размера с сохранением директории хранения и имени. Для этого также необходимо назначить маску *.* в блоке **Маски файлов для поиска**.

Для удобства использования данного режима предусмотрен заранее подготовленный базовый профиль **«Режим разведки»** в плагине «Флешка».

При выборе профиля за исключением «Режима разведки» и отключении флаговой кнопки **Ограничение содержимого файла** файлы будут копироваться полностью.

Выставляя значение в минутах в поле **Таймаут обновления плагина**, оператор задает временной интервал обновления конфигурационных файлов плагина **Флешка**. При наличии загруженной на сервер новой конфигурации для текущего модуля по истечению указанного времени произойдет замена имеющейся конфигурации на сервере.

По окончанию настроек необходимо нажать кнопку **[Назад]** для сохранения введенных настроек и возврата в основное меню настройки плагинов. Отображение кнопки **[Назад]** представлено на рисунке 2.3.1.16.

Настройка плагина завершена. Конфигурация готова к загрузке на сервер.

2.3.1.3 Плагин «Скриншот»

Активируем плагин **Скриншот** путем добавления флажка напротив модуля. Совершаем двойное нажатие левой кнопкой мыши на элемент интерфейса **Скриншот**. Откроется окно с настройками модуля (рисунок 2.3.1.20).

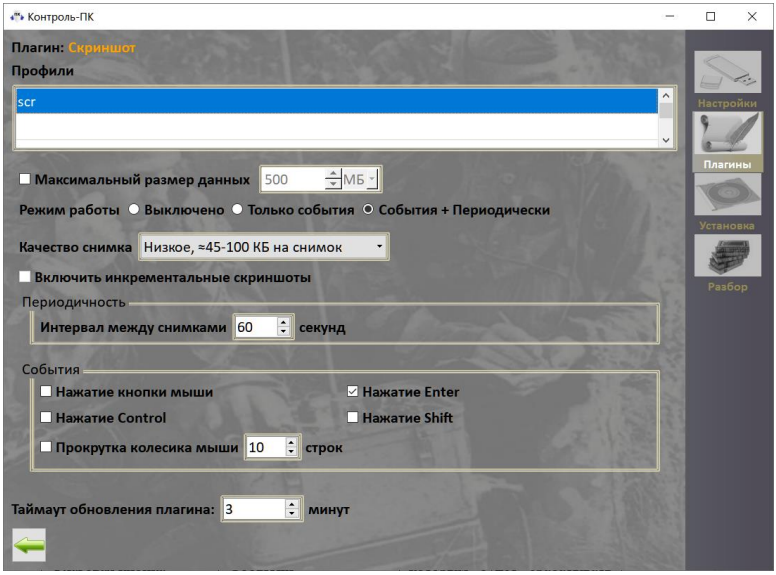

Рисунок 2.3.1.20

В окне настройки плагина **«Скриншот»** (рисунок 2.3.1.20) отображены элементы интерфейса для создания конфигурации модуля, их имена и назначение. Информация представлена в таблице 2.3.1.3.

Таблица 2.3.1.3

Элемент интерфейса	***Имя элемента***	***Назначение***
Таблица данных	**Профили**	Формирование профиля задания
Флаговая кнопка с полем редактирования	**Максимальный размер данных**	Определение верхней границы размера контейнера для сохранения файлов
Радиокнопка	**Выключено**	Определение условия записи снимков с экрана (в данном

Элемент интерфейса	*Имя элемента*	*Назначение*
		положении запись не осуществляется)
Радиокнопка	**Только события**	Определение условия записи снимков с экрана (в данном положении запись осуществляется по событиям)
Радиокнопка	**События + Периодически**	Определение условия записи снимков с экрана (в данном положении запись осуществляется по событиям и заданным временным интервалом между снимками)
Ниспадающее меню	**Качество снимков**	Определение качество записываемых снимков с экрана
Поле редактирования	**Интервал между снимками**	Определение временного интервала между записью снимков с экрана
Флаговая кнопка	**События**	Определение событий, по которым будет срабатывать запись снимков с экрана
Поле редактирования	**Таймаут обновления плагина**	Задание периода обновления конфигурации
Кнопка	**Назад**	Переход в меню «Плагины» с сохранением внесенных изменений

Данный модуль необходим для осуществления сохранения и отправки снимков экрана исследуемого компьютера.

Для настройки плагина **«Скриншот»** необходимо создать новый профиль.

Для создания нового профиля необходимо нажать правую кнопку мыши в свободной строке блока **«Профили»**. Появится предложение **«Добавить»** (рисунок 2.3.1.21).

Рисунок 2.3.1.21

Далее присваиваем имя новому профилю, используя окно ввода данных (рисунок 2.3.1.22).

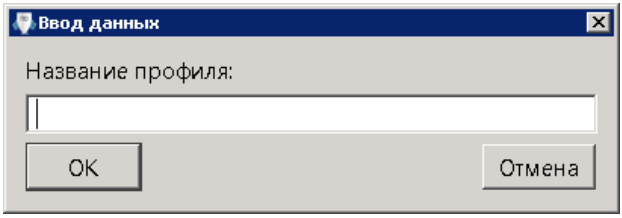

Рисунок 2.3.1.22

Вводим название `Скриншот` и нажимаем **[OK]**. В результате, в блоке **«Профили»** получаем созданный профиль «Скриншот». Отображение профиля на рисунке 2.3.1.23.

Рисунок 2.3.1.23

Также возможно делать копии созданных профилей с дальнейшим изменением копий при необходимости. Инструкция с подробным описанием содержится в разделе 2.3.1.1.

Далее необходимо произвести настройку выбранного профиля. Выбрать созданный профиль «Скриншот».

Активировать флаговую кнопку **Максимальный размер данных** и задать необходимое значение объема отводимого на исследуемом компьютере для сохранения данных (рисунок 2.3.1.24). Единица исчисления также может быть выбрана оператором АРМ.

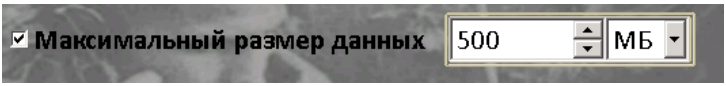

Рисунок 2.3.1.24

Выбран максимальный объем данных *500 мегабайт*. В этом случае при заполнении указанного объема данными агент перестанет накапливать файлы на исследуемом компьютере. В плагине **Скриншот** накопление данных в указанном «контейнере» возможно при отсутствии сетевого соединения с сервером или в случае заполнения свободного объема на жестком диске сервера. В остальных случаях файлы будут отправлены на сервер сразу после появления в «контейнере» на исследуемом компьютере.

При настройке **Режима работы** необходимо выбрать нужную «радиокнопку» (рисунок 2.3.1.25).

Рисунок 2.3.1.25

При выборе режима **Выключено** снимки экрана исследуемого компьютера не будет производиться.

В режиме **Только события** снимок экрана будет произведен при определенных действиях на сервере. О настройке создания снимков по событиям описано ниже.

В режиме **События + Периодически** снимки будут происходить как по определенному действию, так и по истечению определенного интервала времени.

Выбор событий представлен на рисунке 2.3.1.26.

Рисунок 2.3.1.26

Активируя флаговую кнопку **[Нажатие кнопки мыши]**, будет происходить снимок экрана при каждом нажатии кнопки мыши, подключенной к исследуемому компьютеру.

Активируя флаговую кнопку **[Нажатие Enter]**, будет происходить снимок экрана при каждом нажатии клавиши **{Enter}** на клавиатуре, подключенной к исследуемом компьютеру.

Активируя флаговую кнопку **[Нажатие Control]**, будет происходить снимок экрана при каждом нажатии клавиши **{Ctrl** на клавиатуре, подключенной к исследуемом компьютеру.

Активируя флаговую кнопку **[Нажатие Shift]**, будет происходить снимок экрана при каждом нажатии клавиши **{Shift}** на клавиатуре, подключенной к исследуемом компьютеру.

Активируя флаговую кнопку **[Прокрутка колесика мыши]**, будет происходить снимок экрана при совершении пользователем прокрутки колесика мышки, подключенной к исследуемому компьютеру, на указанное количество строк. Количество прокруток необходимое для совершения события указывается в поле для ввода. На рисунке 2.3.1.26 показана конфигурация с прокруткой колесиком 10ти строк.

Настройка периодичности при съемке экрана представлена на рисунке 2.3.1.27.

Рисунок 2.3.127

При данной настройке снимок экрана будет происходить каждые каждые 60 секунд.

Особенность.

Снимки экрана не будут выполняться, если пользователь исследуемого компьютера совершил выход из системы, выполнил выключение компьютера, а также в течение перезагрузки.

При настройке модуля можно выбирать в каком качестве будут происходить снимки экрана. Возможные варианты выбора качества представлены на рисунке 2.3.1.28.

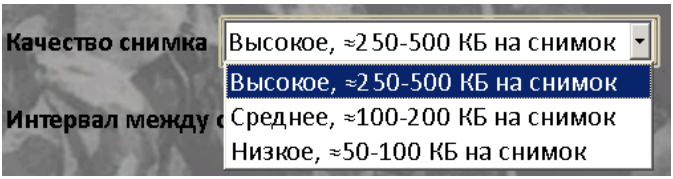

Рисунок 2.3.1.28

Выставляя значение в секундах в поле **Таймаут обновления плагина** (рисунок 2.3.1.21), оператор задает временной интервал обновления конфигурационных файлов плагина **Скриншот**. При наличии загруженной на сервер новой конфигурации для текущего модуля по истечению указанного времени произойдет замена имеющейся конфигурации на сервере.

По окончанию настроек необходимо нажать кнопку **[Назад]** для сохранения введенных настроек и возврата в основное меню настройки плагинов. Отображение кнопки **[Назад]** представлено на рисунке 2.3.1.22.

Настройка плагина завершена. Конфигурация готова к загрузке на сервер.

2.3.1.4 Плагин «Кейлогер»

Активируем плагин **Кейлогер** путем добавления флажка напротив модуля. Совершаем двойное нажатие левой кнопкой мыши на элемент интерфейса **Кейлогер**. Откроется окно с настройками модуля (рисунок 2.3.1.29).

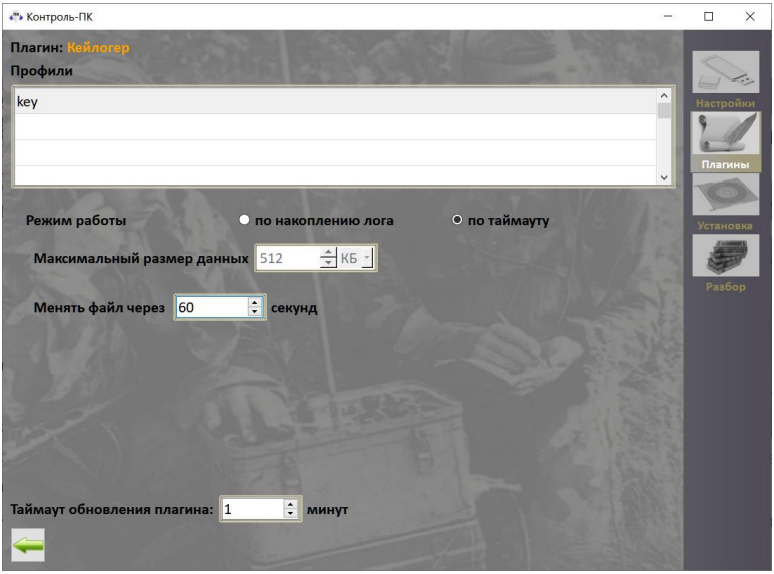

Рисунок 2.3.1.29

В окне настройки плагина **«Кейлогер»** (рисунок 2.3.1.29) отображены элементы интерфейса для создания конфигурации модуля, их имена и назначение. Информация представлена в таблице 2.3.1.4.

Таблица 2.3.1.4

Элемент интерфейса	***Имя элемента***	***Назначение***
Таблица данных	**Профили**	Формирование профиля задания
Радиокнопка	**Выбор режима**	Выбор режима работы модуля
Флаговая кнопка с полем редактирования	**Максимальный размер данных**	Определение максимального размера хранилища для

Элемент интерфейса	*Имя элемента*	*Назначение*
		файлов-журналов событий кейлогера
Флаговая кнопка с полем редактирования	**Менять файл через**	Определение времени создания нового файла с событиями от кейлогера
Поле редактирования	**Таймаут обновления плагина**	Задание периода обновления конфигурации
Кнопка	**Назад**	Переход в меню «Плагины» с сохранением внесенных изменений

Данный модуль необходим для осуществления сохранения и отправления файлов содержанием которых является набор клавиатурных последовательностей, вводимых пользователем исследуемого компьютера.

Для настройки плагина **«Кейлогер»** необходимо создать новый профиль (рисунок 2.3.1.30)

Рисунок 2.3.1.30

Для создания нового профиля необходимо нажать правую кнопку мыши в свободной строке блока **«Профили»**. Появится предложение **«Добавить»** (рисунок 2.3.1.31).

Рисунок 2.3.1.31

Далее присваиваем имя новому профилю, используя окно ввода данных (рисунок 2.3.1.32).

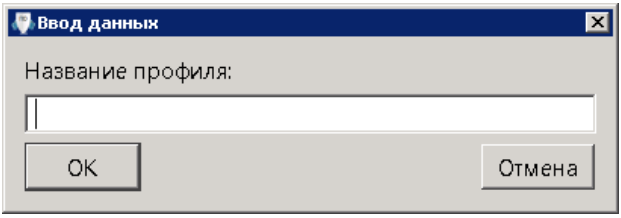

Рисунок 2.3.1.32

Вводим название `Кейлогер` и нажимаем **[OK]**. В результате, в блоке **«Профили»** получаем созданный профиль «Кейлогер». Отображение профиля на рисунке 2.3.1.33

Рисунок 2.3.1.33

Также возможно делать копии созданных профилей с дальнейшим изменением копий при необходимости. Инструкция с подробным описанием содержится в разделе 2.3.1.1.

Далее необходимо произвести настройку выбранного профиля. Выбрать созданный профиль «Кейлогер». Далее выбрать режим работы модуля.

Выбрав режим работы **по накоплению лога**, необходимо задать **Максимальный размер данных** - необходимое значение объема отводимого на исследуемом компьютере для сохранения данных (рисунок 2.3.1.34). Единица исчисления также может быть выбрана оператором АРМ.

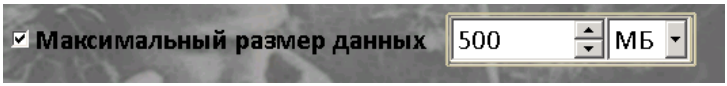

Рисунок 2.3.1.34

Выбран максимальный объем данных *500 мегабайт*. В этом случае при заполнении указанного объема данными агент перестанет накапливать файлы на исследуемом компьютере. В плагине **Кейлогер** накопление данных в указанном «контейнере» возможно при отсутствии сетевого соединения с сервером или в случае заполнении свободного объема на жестком диске сервера. В остальных случаях файлы будут отправлены на сервер сразу после появления в «контейнере» на исследуемом компьютере.

При выборе режима по таймауту, необходимо установить временное значение **Менять файл через** в секундах (рисунок 2.3.1.35).

Рисунок 2.3.1.35

При активации данного поля по умолчанию введено значение *3600 секунд*. По истечению этого интервала файл с накопленными клавиатурными нажатиями будет отправлен на сервер.

Особенность.

Клавиатурные нажатия будут работать при условии ввода только с клавиатуры, подключенной напрямую к исследуемому компьютеру.

Выставляя значение в секундах в поле **Таймаут обновления плагина** (рисунок 2.3.1.21), оператор задает временной интервал обновления конфигурационных файлов плагина **Кейлогер**. При наличии загруженной на сервер новой конфигурации для текущего модуля по истечению указанного времени произойдет замена имеющейся конфигурации на сервере.

По окончанию настроек необходимо нажать кнопку **[Назад]** для сохранения введенных настроек и возврата в основное меню настройки плагинов. Отображение кнопки **[Назад]** представлено на рисунке 2.3.1.22.

Настройка плагина завершена. Конфигурация готова к загрузке на сервер.

2.3.2 Загрузка задания

Настроенные плагины необходимо загрузить на сервер. Для этого используем следующий блок с функционалом вкладки **Плагины** (рисунок 2.3.2.1)

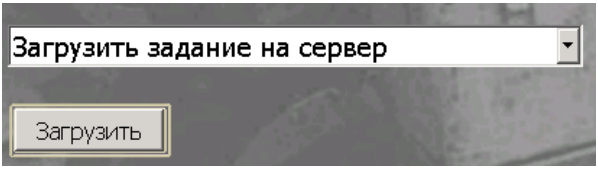

Рисунок 2.3.2.1

При нажатии на кнопку **[Загрузить задание на сервер]** произойдет загрузка ранее сконфигурированных модулей на сервер. Для успешной загрузки необходимо провести корректную настройку агента в окне **Настройки**. Перед загрузкой программа отобразит окно с подтверждением загрузки и введенных параметров модулей. На рисунке 2.3.2.2 отображен пример окна с подтверждением для плагина «Скриншот». Нажимаем кнопку **[Подтвердить]** для дальнейшей загрузки или **[Отмена]** для внесения необходимых изменений в конфигурацию модулей. Подробное описание строк в окне **Подтверждение загрузки** описано в индивидуальных настройках каждого плагина.

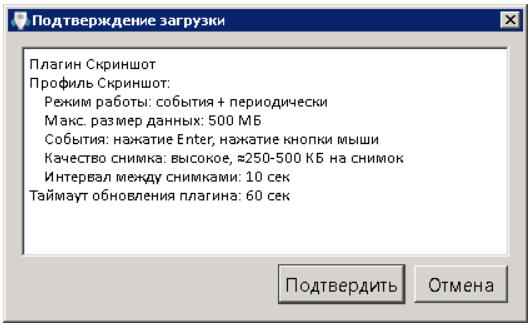

Рисунок 2.3.2.2

Процесс загрузки заданий на сервер отображен на рисунке 2.3.2.3.

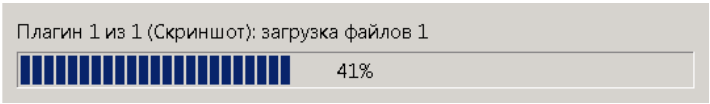

Рисунок 2.3.2.3

По окончанию загрузки программа отобразит следующее окно (рисунок 2.3.2.4):

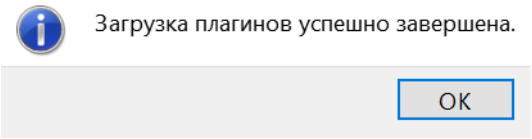

Рисунок 2.3.2.4

Данные успешно загружены на сервер.

2.4 Установка агента

Для совершения операции установки программы необходимо перейти на вкладку **Установка** (рисунок 2.4.1), расположенную в правой части окна программы. Предварительно потребуется выполнить настройки конфигурации агента. Также потребуется сформировать и загрузить задание для работы агента. Шаги по необходимой настройке описаны в разделе 2.2 и 2.3.

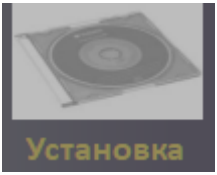

Рисунок 2.4.1

При переходе на вкладку **Установка** отобразится следующее окно (рисунок 2.4.2).

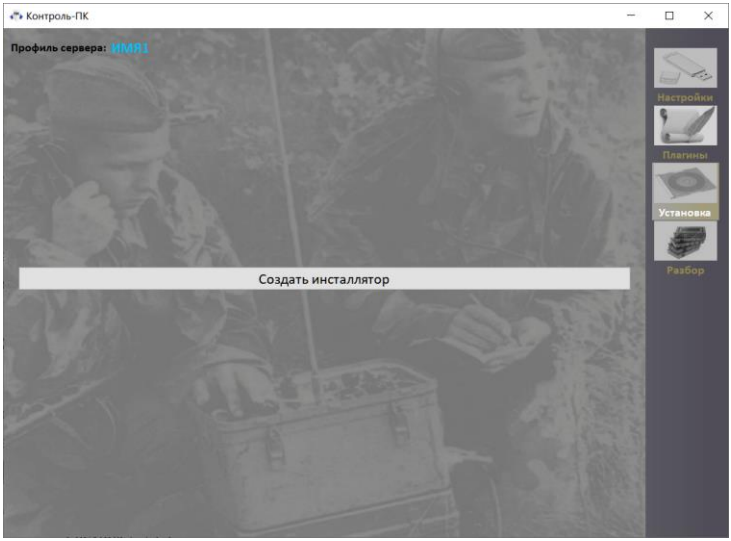

Рисунок 2.4.2

Одним из элементов на вкладке **Установка** является информационная панель (рисунок 2.4.3) с указанием выбранного профиля сервера. Операции по настройке и выбор профиля описаны в разделе 2.2.1.1. При нажатии на выбранный профиль (*ИМЯ1*) программа переключится на вкладку **Настройки** для уточнения или изменения настроек сервера.

Рисунок 2.4.3

К основным операциям при работе с вкладкой **Установка** относятся операции по созданию программы-инсталлятора агента.

Для установки агента через исполняемую программу необходимо перейти на вкладку **Установка**, затем нажать кнопку **[Создать инсталлятор]** (рисунок 2.4.4).

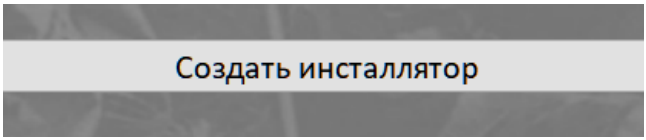

Рисунок 2.4.4

АРМ оператора выгрузит два файла. В процессе создания необходимо дождаться появления окна **«Создание инсталлятора успешно завершено»** (рисунок 2.4.5) и нажать кнопку **[OK]**.

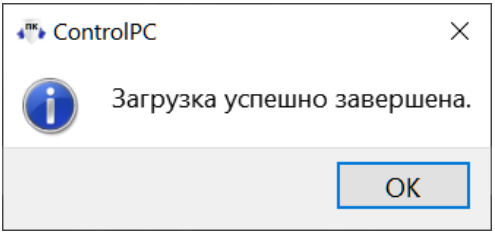

Рисунок 2.4.5

Подготовленные файлы необходимо записать на флеш-носитель. После успешной записи, флеш-носитель необходимо извлечь из исследующего компьютера.

Следующие шаги требуются по установке агента на исследуемый компьютер:

1. Необходимо подключить подготовленный флеш-носитель к исследуемому компьютеру;
2. Запустить исполняемую программу Installer.exe с флеш-носителя и подождать в течение 10 секунд;
3. Извлечь флеш-носитель из компьютера;
4. Выполнить перезагрузку исследуемого компьютера.

Внимание!

Установка агента производится в операционные системы, установленные на исследуемые компьютеры с отключенными или не установленными антивирусными средствами!

2.5 Копирование и распаковывание данных

Для копирования и распаковывания данных из исследуемого компьютера используется функционал вкладки **Разбор** (рисунок 2.5.1).

Рисунок 2.5.1

В этом разделе описаны операции по загрузке и распаковыванию данных напрямую с сервера и с локального источника. Описана возможность выбора директории для разбора. Внешний вид окна **Разбор** представлен на рисунке 2.5.2.

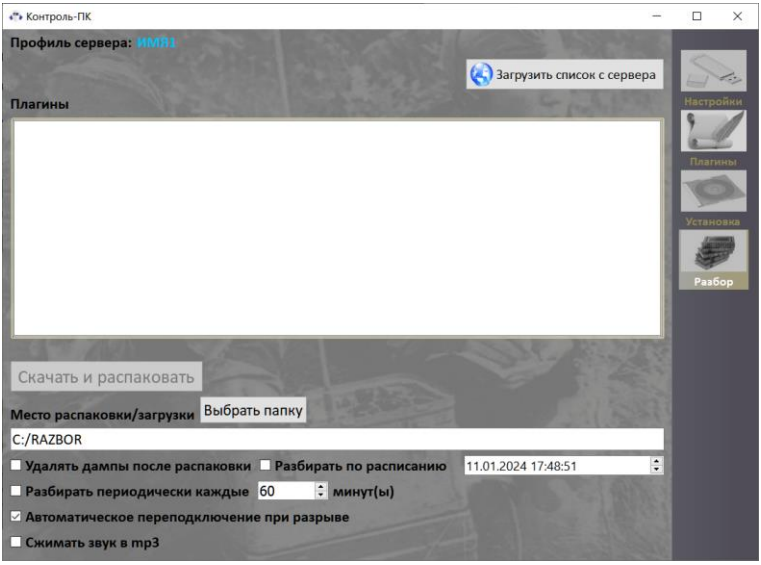

Рисунок 2.5.2

Элементы интерфейса окна **Разбор**, их имена и назначение представлены в таблице 2.5.1

Таблица 2.5.1.

Элемент интерфейса	***Имя элемента***	***Назначение***
Кнопка	**Загрузить список с сервера**	Загрузка списка данных с сервера.

Элемент интерфейса	*Имя элемента*	*Назначение*
Таблица данных	**Плагины**	Вывод списка включенных в задание плагинов с собранными данными.
Кнопка с полем редактирования	**Выбрать папку**	Выбор директории для распаковывания данных
Флаговая кнопка	**Удалять дампы после распаковки**	Включение возможности удаления распакованных данных.
Кнопка	**Скачать и распаковать**	Скачивание и распаковывание данных.
Флаговая кнопка	**Автоматическое переподключение при разрыве**	Включение возможности переподключения для дальнейшего разбора данных с места прерывания.
Флаговая кнопка	**Разбирать периодически каждые**	Включение возможности автоматической распаковки с указанным интервалом.
Флаговая кнопка	**Разбирать по расписанию**	Включение возможности автоматической распаковки в указанное время.
Флаговая кнопка	**Сжимать звук в MP3**	Включение возможности распаковки звука в формате mp3

Одним из элементов на вкладке **Разбор** является информационная панель (рисунок 2.5.3) с указанием выбранного профиля сервера. Операции по настройке и выбор профиля описаны в разделе 2.2.1.1. При нажатии на профиль сервера (*ИМЯ1*) программа переключится на вкладку **Настройки** для уточнения или изменения настроек сервера.

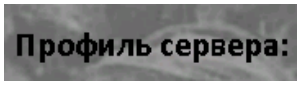

Рисунок 2.5.3

На случай обрыва сетевого соединения в момент загрузки и распаковывания данных в программе предусмотрена возможность автоматического подключения к серверу с целью продолжения разбора данных. Отображение функционала на рисунке 2.5.4.

Рисунок 2.5.4

2.5.1 Загрузка списка данных

Для загрузки данных необходимо нажать кнопку **[Загрузить список с сервера]**, дождаться окончания процесса загрузки списка данных с HTTPS-сервера. Далее в окне **Плагины** на вкладке **Разбор** будет представлен список плагинов, включенных в задание.

При нажатии на **[Загрузить список с сервера]** будет выведено следующее окно (рисунок 2.5.1.1):

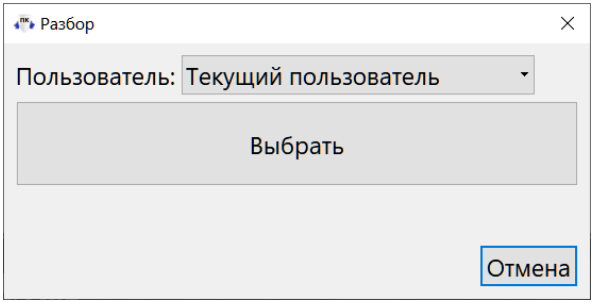

Рисунок 2.5.1.1

Оператору представлена возможность выбрать пользователя согласно тому, какую директорию мероприятия необходимо распаковать.

Если на данный момент соединение с сервером отсутствует, то появится следующее сообщение (рисунок 2.5.1.2)

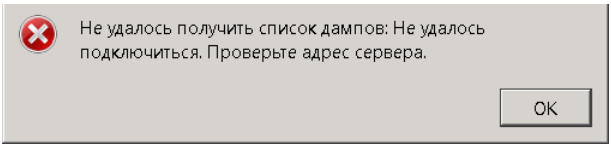

Рисунок 2.5.1.2

При неправильно введенных данных пользователя появится следующее сообщение об ошибке (рисунок 2.5.1.3)

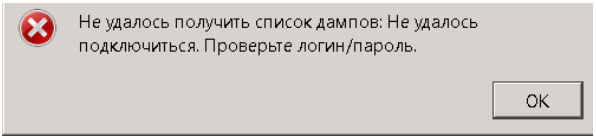

Рисунок 2.5.1.3

На рисунке 2.5.1.4 представлен процесс получения списка модулей с сервера.

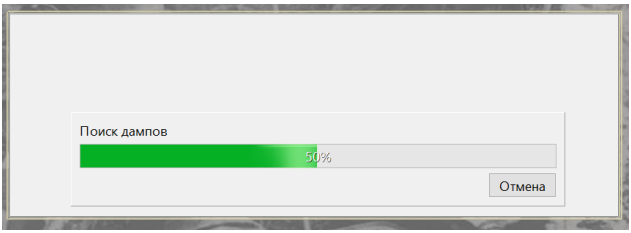

Рисунок 2.5.1.4

При нажатии на кнопку **[Отмена]** появится диалоговое окно (рисунок 2.5.1.5). На этом шаге можно отменить загрузку списка модулей или продолжить его получение.

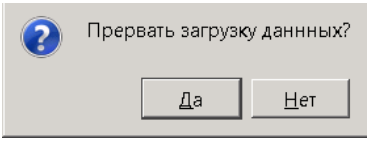

Рисунок 2.5.1.5

Результат поиска представлен на рисунке 2.5.1.6.

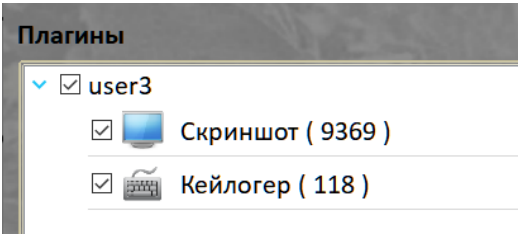

Рисунок 2.5.1.6

2.5.2 Распаковывание данных

После того, как список плагинов с данными загружен можно приступить к выбору директории для полного или частичного разбора данных.

Необходимо нажать на кнопку **[Выбрать папку]** и указать директорию на локальном хранилище рабочего места оператора (рисунок 2.5.2.1)

Рисунок 2.5.2.1

Для частичного разбора данных необходимо выбрать необходимый для разбора плагин. Действие произвести в таблице **Плагины** во вкладке **Разбор** (рисунок 2.5.2.2).

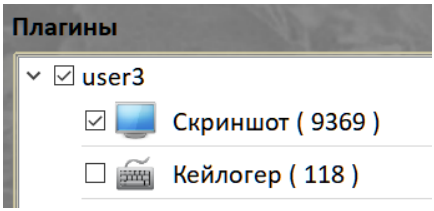

Рисунок 2.5.2.2

На рисунке представлен выбор места распаковки и требуемый для разбора плагин «Скриншот». Далее нажимаем на кнопку **[Распаковать]** ждем завершения процесса.

Графическое представление процесса разбора представлено на рисунке 2.5.2.3.

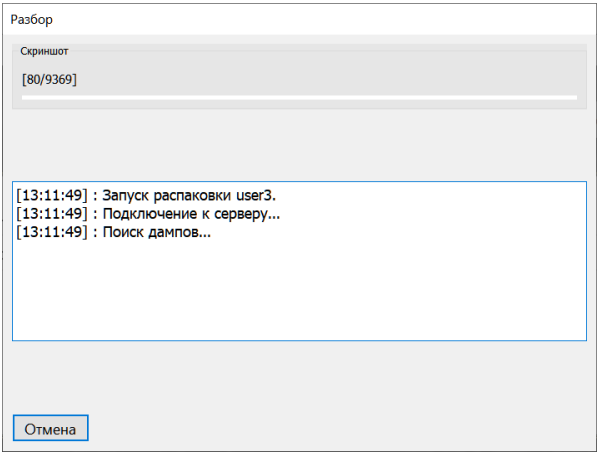

Рисунок 2.5.2.3

Также в функционале программы предусмотрен **режим пофайлового разбора**. Для этого по выбранному плагину необходимо совершить двойной клик левой кнопкой мыши. Откроется окно для выбора пофайлового разбора (рисунок 2.5.2.4).

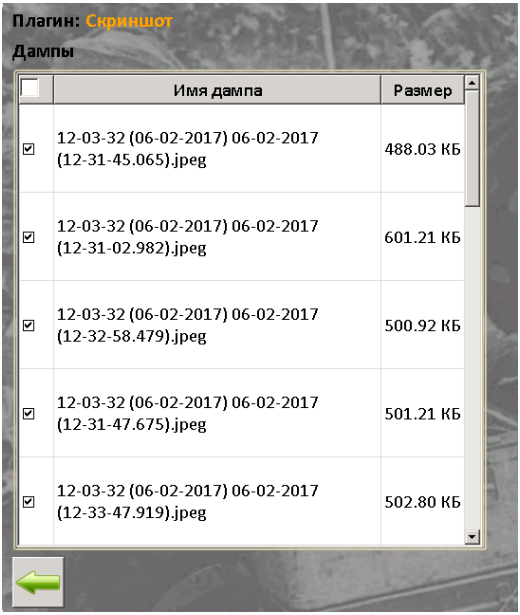

Рисунок 2.5.2.4

Выделяем необходимый файл или группу файлов, затем нажимаем на кнопку **[Назад]**, при этом возвратимся в предыдущее окно и нажимаем на кнопку **[Распаковать]**. Ждем завершения процесса.

Для полного разбора данных выбираем все доступные для разбора модули и нажимаем на кнопку **[Распаковать]**.

Необходимо дождаться окончания процесса разбора.

На следующем рисунке 2.5.2.5 представлено содержание папки Скриншоты, а на рисунке 2.5.2.6 пример сделанного скриншота, совершенного по действию.

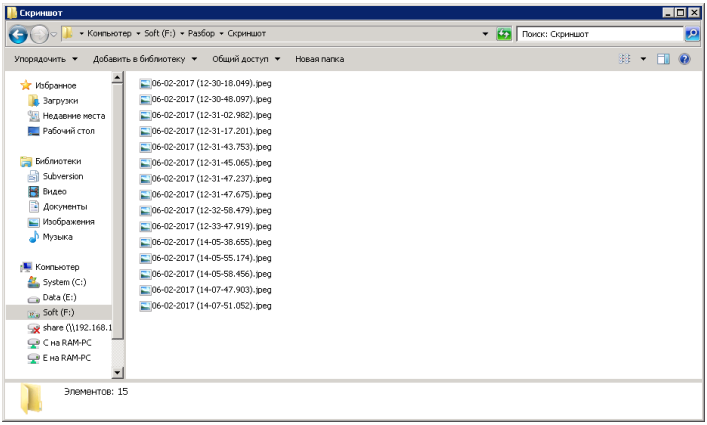

Рисунок 2.5.2.5

Рисунок 2.5.2.6

В случае, если после распаковывания потребуется удаление распакованных данных, то необходимо установить флажок **«Удалять файлы с сервера после распаковки»** (рисунок 2.5.2.7) перед тем, как нажать на кнопку **[Распаковать]**.

Рисунок 2.5.2.7

2.6 Удаление агента

Удаление агента может осуществляться средствами управляющего модуля «Контроль-ПК» на исследуемом компьютере.

Для удаления модулей без удаления самого агента необходимо перейти на вкладку **Плагины**, далее нажать на кнопку **[Команды]** (рисунок 2.6.1).

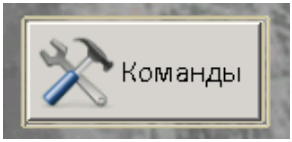

Рисунок 2.6.1

Откроется окно (рисунок 2.6.2) с отображением возможных команд управления. Необходимо выбрать одну из представленных команд и нажать **[Выполнить]**.

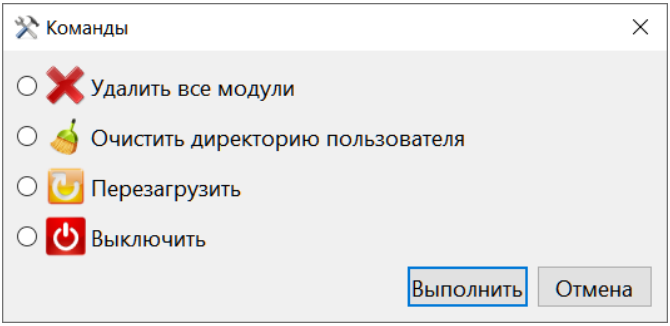

Рисунок 2.8.2

При нажатии кнопки **[Выполнить]** произойдет отправка выбранной команды на сервер. При получении команды на сервер последует действие, соответствующее выбранной команде. При нажатии кнопки **[Отмена**], окно **Команды** закроется и станет активным окно вкладки **Плагины**.

Выполнение команды «Удалить все модули» позволяет приостановить функционирование всех активных плагинов. Для возобновления работы плагинов необходимо заново загрузить задания на сервер, используя установленную на АРМ оператора программу «Контроль-ПК». После выполнения команды подход к исследуемому компьютеру не требуется.

Выполнение команды «Очистить директорию пользователя» позволяет удалить содержимое директории «output». В этом случае накопленная информация по выбранному в Настройках пользователю будет удалена. Подробнее о структуре директорий сервера описано в разделе 2.5.

Если выполнить команду «Перезагрузить», то произойдет перезагрузка операционной системы, установленной на исследуемый компьютер.

При выполнении команды «Выключить» произойдет выключение операционной системы на исследуемом компьютере.

Внимание!

Все действия с командами будут успешно производиться только при наличии работающего в данный момент агента на исследуемом компьютере.

Для удаления агента необходимо скопировать uninstaller.exe из корневой директории uninstaller на USB накопитель.

Далее потребуется подключить накопитель к исследующему ПК и запустить uninstaller.exe.

Повторное возобновление работы на данном исследуемом компьютере без дополнительных необходимых действий оператора станет невозможно.

Скрытие и выход из программы

Для скрытия окон программы с экрана монитора на панели инструментов нажмите на графический элемент **[Свернуть]**, расположенный в правом верхнем углу окна программы (рисунок 2.9.1).

Рисунок 2.9.1

После нажатия, главное окно программы не будет отображаться на экране монитора.

1. Для восстановления главного окна программы на экране монитора на панели задач нажмите на иконку Контроль-ПК (рисунок 2.9.2).

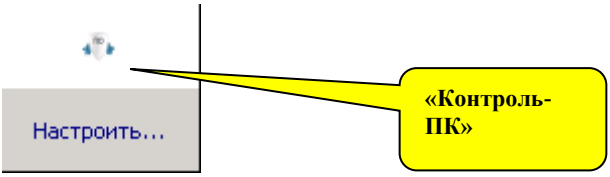

Рисунок 09.2

Главное окно программы будет восстановлено на экране монитора.

Для выхода из программы в главном окне на панели инструментов нажмите на кнопку **[Закрыть]** (рисунок 2.9.1).

Процесс работы с комплексом считается завершенным.